

## 8. Physical and Cyber Security Aspects of the Blackout

### Summary

The objective of the Security Working Group (SWG) is to determine what role, if any, that a malicious cyber event may have played in causing, or contributing to, the power outage of August 14, 2003. Analysis to date provides no evidence that malicious actors are responsible for, or contributed to, the outage. The SWG acknowledges reports of al-Qaeda claims of responsibility for the power outage of August 14, 2003; however, those claims are not consistent with the SWG's findings to date. There is also no evidence, nor is there any information suggesting, that viruses and worms prevalent across the Internet at the time of the outage had any significant impact on power generation and delivery systems. SWG analysis to date has brought to light certain concerns with respect to: the possible failure of alarm software; links to control and data acquisition software; and the lack of a system or process for some operators to view adequately the status of electric systems outside their immediate control.

Further data collection and analysis will be undertaken by the SWG to test the findings detailed in this interim report and to examine more fully the cyber security aspects of the power outage. The outcome of Electric System Working Group (ESWG) root cause analysis will serve to focus this work. As the significant cyber events are identified by the ESWG, the SWG will examine them from a security perspective.

### Security Working Group: Mandate and Scope

It is widely recognized that the increased reliance on information technology (IT) by critical infrastructure sectors, including the energy sector, has increased their vulnerability to disruption via cyber means. The ability to exploit these vulnerabilities has been demonstrated in North America. The SWG was established to address the cyber-related aspects of the August 14, 2003, power outage. The SWG is made up of U.S. and

Canadian Federal, State, Provincial, and local experts in both physical and cyber security. For the purposes of its work, the SWG has defined a "malicious cyber event" as the manipulation of data, software or hardware for the purpose of deliberately disrupting the systems that control and support the generation and delivery of electric power.

The SWG is working closely with the U.S. and Canadian law enforcement, intelligence, and homeland security communities to examine the possible role of malicious actors in the power outage of August 14, 2003. A primary activity to date has been the collection and review of available intelligence that may relate to the outage.

The SWG is also collaborating with the energy industry to examine the cyber systems that control power generation and delivery operations, the physical security of cyber assets, cyber policies and procedures, and the functionality of supporting infrastructures-such as communication systems and backup power generation, which facilitate the smooth-running operation of cyber assets-to determine whether the operation of these systems was affected by malicious activity. The collection of information along these avenues of inquiry is ongoing.

The SWG is coordinating its efforts with those of the other Working Groups, and there is a significant interdependence on the work products and findings of each group. The SWG's initial focus is on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG. The outcome of ESWG analysis will serve to identify key events that may have caused, or contributed to, the outage. As the significant cyber events are identified, the SWG will examine them from a security perspective. The amount of information for analysis is identified by the ESWG as pertinent to the SWG's analysis is considerable.

Examination of the physical, non-cyber infrastructure aspects of the power outage of August 14, 2003, is outside the scope of the SWG's analysis.

Nevertheless, if a breach of physical security unrelated to the cyber dimensions of the infrastructure comes to the SWG's attention during the course of the work of the Task Force, the SWG will conduct the necessary analysis.

Also outside the scope of the SWG's work is analysis of the cascading impacts of the power outage on other critical infrastructure sectors. Both the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and the U.S. Department of Homeland Security (DHS) are examining these issues, but not within the context of the Task Force. The SWG is closely coordinating its efforts with OCIPEP and DHS.

## **Cyber Security in the Electricity Sector**

The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting the electric power system. Even attacks that do not directly target the electricity sector can have disruptive effects on electricity system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications. One such incident occurred in January 2003, when the "Slammer" Internet worm took down monitoring computers at FirstEnergy Corporation's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council (NERC) concluded that, although it caused no outages, the infection blocked commands that operated other power utilities. The report, "NRC Issues Information Notice on Potential of Nuclear Power Plant Network to Worm Infection," is available at web site <http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html>.

This example, among others, highlights the increased vulnerability to disruption via cyber means faced by North America's critical infrastructure sectors, including the energy sector. Of specific concern to the U.S. and Canadian governments are the Supervisory Control and Data Acquisition (SCADA) systems, which contain computers and applications that perform a wide variety of functions across many industries. In electric power, SCADA includes telemetry for status and control, as well as Energy Management Systems (EMS), protective relaying, and automatic generation control. SCADA systems were

developed to maximize functionality and interoperability, with little attention given to cyber security. These systems, many of which were intended to be isolated, are now, for a variety of business and operational reasons, either directly or indirectly connected to the global Internet. For example, in some instances, there may be a need for employees to monitor SCADA systems remotely. However, connecting SCADA systems to a remotely accessible computer network can present security risks. These risks include the compromise of sensitive operating information and the threat of unauthorized access to SCADA systems' control mechanisms.

Security has always been a priority for the electricity sector in North America; however, it is a greater priority now than ever before. Electric system operators recognize that the threat environment is changing and that the risks are greater than in the past, and they have taken steps to improve their security postures. NERC's Critical Infrastructure Protection Advisory Group has been examining ways to improve both the physical and cyber security dimensions of the North American power grid. This group includes Canadian and U.S. industry experts in the areas of cyber security, physical security and operational security. The creation of a national SCADA program to improve the physical and cyber security of these control systems is now also under discussion in the United States. The Canadian Electrical Association Critical Infrastructure Working Group is examining similar measures.

## **Information Collection and Analysis**

In addition to analyzing information already obtained from stakeholder interviews, telephone transcripts, law enforcement and intelligence information, and other ESWG working documents, the SWG will seek to review and analyze other sources of data on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG. Available information includes log data from routers, intrusion detection systems, firewalls, and EMS; change management logs; and physical security materials. Data are currently being collected, in collaboration with the private sector and with consideration toward its protection from further disclosure where there are proprietary or national security concerns.

The SWG is divided into six sub-teams to address the discrete components of this investigation: Cyber Analysis, Intelligence Analysis, Physical Analysis, Policies and Procedures, Supporting Infrastructure, and Root Cause Liaison. The SWG organized itself in this manner to create a holistic approach to each of the main areas of concern with regard to power grid vulnerabilities. Rather than analyze each area of concern separately, the SWG sub-team structure provides a more comprehensive framework in which to investigate whether malicious activity was a cause of the power outage of August 14, 2003. Each sub-team is staffed with Subject Matter Experts (SMEs) from government, industry, and academia to provide the analytical breadth and depth necessary to complete its objective. A detailed overview of the sub-team structure and activities, those planned and those taken, for each sub-team is provided below.

## Cyber Analysis

The Cyber Analysis sub-team is led by the CERT® Coordination Center (CERT/CC) at Carnegie Mellon University and the Royal Canadian Mounted Police (RCMP). This team is focused on analyzing and reviewing the electronic media of computer networks in which online communications take place. The sub-team is examining these networks to determine whether they were maliciously used to cause, or contribute to, the August 14 outage. It is specifically reviewing the existing cyber topology, cyber logs, and EMS logs. The team is also conducting interviews with vendors to identify known system flaws and vulnerabilities. The sub-team is collecting, processing, and synthesizing data to determine whether a malicious cyber-related attack was a direct or indirect cause of the outage.

This sub-team has taken a number of steps in recent weeks, including reviewing NERC reliability standards to gain a better understanding of the overall security posture of the electric power industry. Additionally, the sub-team participated in meetings in Baltimore on August 22 and 23, 2003. The meetings provided an opportunity for the cyber experts and the power industry experts to understand the details necessary to conduct an investigation. The cyber data retention request was produced during this meeting.

Members of the sub-team also participated in the NERC/Department of Energy (DOE) Fact Finding meeting held in Newark, New Jersey, on September 8, 2003. Each company involved in the outage

provided answers to a set of questions related to the outage. The meeting helped to provide a better understanding of what each company experienced before, during, and after the outage. Additionally, sub-team members participated in interviews with the control room operators from FirstEnergy on October 8 and 9, 2003, and from Cinergy on October 10, 2003. These interviews have identified several key areas for further discussion.

The Cyber Analysis sub-team continues to gain a better understanding of events on August 14, 2003. Future analysis will be driven by information received from the ESWG's Root Cause Analysis sub-team and will focus on:

- ◆ Conducting additional interviews with control room operators and IT staff from the key companies involved in the outage.
- ◆ Conducting interviews with the operators and IT staff responsible for the NERC Interchange Distribution Calculator system. Some reports indicate that this system may have been unavailable during the time of the outage.
- ◆ Conducting interviews with key vendors for the EMS.
- ◆ Analyzing the configurations of routers, firewalls, intrusion detection systems, and other network devices to get a better understanding of potential weaknesses in the control system cyber defenses.
- ◆ Analyzing logs and other information for signs of unauthorized activity.

## Intelligence Analysis

The Intelligence Analysis sub-team is led by DHS and the RCMP, which are working closely with Federal, State, and local law enforcement, intelligence, and homeland security organizations to assess whether the power outage was the result of a malicious attack. Preliminary analysis provides no evidence that malicious actors—either individuals or organizations—are responsible for, or contributed to, the power outage of August 14, 2003. Additionally, the sub-team has found no indication of deliberate physical damage to power generating stations and delivery lines on the day of the outage, and there are no reports indicating that the power outage was caused by a computer network attack.

Both U.S. and Canadian government authorities provide threat intelligence information to their respective energy sectors when appropriate. No



intelligence reports before, during, or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature relating to the sector, which was provided to the North American energy industry by U.S. and Canadian government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack involving explosions at oil production facilities, power plants, or nuclear plants on the U.S. East Coast during the summer of 2003. The type of physical attack described in the intelligence that prompted this threat warning is not consistent with the events of the power outage; there is no indication of a kinetic event before, during, or immediately after the August 14 outage.

Despite all the above indications that no terrorist activity caused the power outage, al-Qaeda did publicly claim responsibility for its occurrence:

◆ **August 18, 2003:** Al-Hayat, an Egyptian media outlet, published excerpts from a communiqué attributed to al-Qaeda. Al Hayat claimed to have obtained the communiqué from the website of the International Islamic Media Center. The content of the communiqué asserts that the “brigades of Abu Fahes Al Masri had hit two main power plants supplying the East of the U.S., as well as major industrial cities in the U.S. and Canada, ‘its ally in the war against Islam (New York and Toronto) and their neighbors.’” Furthermore, the operation “was carried out on the orders of Osama bin Laden to hit the pillars of the U.S. economy,” as “a realization of bin Laden’s promise to offer the Iraqi people a present.” The communiqué does not specify the way in which the alleged sabotage was carried out, but it does elaborate on the alleged damage to the U.S. economy in the areas of finance, transportation, energy, and telecommunications.

Additional claims and commentary regarding the power outage appeared in various Middle Eastern media outlets:

◆ **August 26, 2003:** A conservative Iranian daily newspaper published a commentary regarding the potential of computer technology as a tool for terrorists against infrastructures dependent on computer networks—most notably, water, electric, public transportation, trade organizations, and “supranational companies” in the United States.

◆ **September 4, 2003:** An Islamist participant in a Jihadist chat room forum claimed that sleeper

cells associated with al-Qaeda used the power outage as a cover to infiltrate the United States from Canada.

These claims above, as known, are not consistent with the SWG’s findings to date. They are also not consistent with recent congressional testimony by the U.S. Federal Bureau of Investigation (FBI). Larry A. Mefford, Executive Assistant Director in charge of the FBI’s Counterterrorism and Counterintelligence programs, testified to the U.S. Congress on September 4, 2003, that, “To date, we have not discovered any evidence indicating that the outage was a result of activity by international or domestic terrorists or other criminal activity.” He also testified that, “The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past and the claim of the Abu Hafs al-Masri Brigade to have caused the blackout appears to be no more than wishful thinking. We have no information confirming the actual existence of this group.” Mr. Mefford’s Statement for the Record is available at web site <http://www.fbi.gov/congress/congress03/mefford090403.htm>.

Current assessments suggest that there are terrorists and other malicious actors who have the capability to conduct a malicious cyber attack with potential to disrupt the energy infrastructure. Although such an attack cannot be ruled out entirely, an examination of available information and intelligence does not support any claims of a deliberate attack against the energy infrastructure on, or leading up to, August 14, 2003. The few instances of physical damage that occurred on power delivery lines were the result of natural acts and not of sabotage. No intelligence reports before, during, or after the power outage indicate any specific terrorist plans or operations against the energy infrastructure. No incident reports detail suspicious activity near the power generation plants or delivery lines in question.

## Physical Analysis

The Physical Analysis sub-team is led by the U.S. Secret Service and the RCMP. These organizations have particular expertise in physical security assessments in the energy sector. The sub-team is focusing on issues related to how the cyber-related facilities of the energy sector companies are secured, including the physical integrity of data centers and control rooms, along with security procedures and policies used to limit access to sensitive areas. Focusing on the facilities identified as having a causal relationship to the outage,

the sub-team is seeking to determine whether the physical integrity of the cyber facilities was breached, either externally or by an insider, before or during the outage; and if so, whether such a breach caused or contributed to the power outage. Although the sub-team has analyzed information provided to both the EWG and the Nuclear Working Group (NWG), the Physical Analysis sub-team is also reviewing information resulting from recent face-to-face meetings with energy sector personnel and site visits to energy sector facilities, to determine the physical integrity of the cyber infrastructure.

The sub-team has compiled a list of questions covering location, accessibility, cameras, alarms, locks, and fire protection and water systems as they apply to computer server rooms. Based on discussions of these questions during its interviews, the sub-team is in the process of ascertaining whether the physical integrity of the cyber infrastructure was breached. Additionally, the sub-team is examining access and control measures used to allow entry into command and control facilities and the integrity of remote facilities.

The sub-team is also concentrating on mechanisms used by the companies to report unusual incidents within server rooms, command and control rooms, and remote facilities. The sub-team is also addressing the possibility of an insider attack on the cyber infrastructure.

## **Policies and Procedures**

The Policies and Procedures sub-team is led by DHS and OCIPEP, which have personnel with strong backgrounds in the fields of electric delivery operations, automated control systems (including SCADA and EMS), and information security. The sub-team is focused on examining the overall policies and procedures that may or may not have been in place during the events leading up to and during the August 14 power outage. The team is examining policies that are centrally related to the cyber systems of the companies identified in the early stages of the power outage. Of specific interest are policies and procedures regarding the upgrade and maintenance (to include system patching) of the command and control (C2) systems, including SCADA and EMS. Also of interest are the procedures for contingency operations and restoration of systems in the event of a computer system failure or a cyber event, such as an active hack or the discovery of malicious code. The group is conducting further interviews

and is continuing its analysis to build solid conclusions about the policies and procedures relating to the outage.

## **Supporting Infrastructure**

The Supporting Infrastructure sub-team is led by a DHS expert with experience assessing supporting infrastructure elements such as water cooling for computer systems, backup power systems, heating, ventilation and air conditioning (HVAC), and supporting telecommunications networks. OCIPEP is the Canadian co-lead for this effort. The sub-team is analyzing the integrity of the supporting infrastructure and its role, if any, in the August 14 power outage, and whether the supporting infrastructure was performing at a satisfactory level before and during the outage. In addition, the team is contacting vendors to determine whether there were maintenance issues that may have affected operations during or before the outage.

The sub-team is focusing specifically on the following key issues in visits to each of the designated electrical entities:

- ◆ Carrier/provider/vendor for the supporting infrastructure services and/or systems at select company facilities
- ◆ Loss of service before and/or after the power outage
- ◆ Conduct of maintenance activities before and/or after the power outage
- ◆ Conduct of installation activities before and/or after the power outage
- ◆ Conduct of testing activities before and/or after the power outage
- ◆ Conduct of exercises before and/or after the power outage
- ◆ Existence of a monitoring process (log, checklist, etc.) to document the status of supporting infrastructure services.

## **Root Cause Analysis**

The SWG Root Cause Liaison sub-team (SWG/RC) has been following the work of the ESWG to identify potential root causes of the power outage. As these root cause elements are identified, the sub-team will assess with the ESWG any potential linkages to physical and/or cyber malfeasance.

The root cause analysis work of the ESWG is still in progress; however, the initial analysis has

found no causal link between the power outage and malicious activity, whether physical or cyber initiated. Root cause analysis for an event like the August 14 power outage involves a detailed process to develop a hierarchy of actions and events that suggest causal factors. The process includes: development of a detailed timeline of the events, examination of actions related to the events, and an assessment of factors that initiated or exacerbated the events. An assessment of the impact of physical security as a contributor to the power outage is conditional upon discovery of information suggesting that a malicious physical act initiated or exacerbated the power outage. There are no such indications thus far, and no further assessment by the SWG in this area is indicated.

## Cyber Timeline

The following sequence of events was derived from discussions with representatives of FirstEnergy and the Midwest Independent Transmission System Operator (MISO). All times are approximate and will need to be confirmed by an analysis of company log data.

- ◆ The first significant cyber-related event of August 14, 2003, occurred at 12:40 EDT at the MISO. At this time, a MISO EMS engineer purposely disabled the automatic periodic trigger on the State Estimator (SE) application, which allows MISO to determine the real-time state of the power system for its region. Disabling of the automatic periodic trigger, a program feature that causes the SE to run automatically every 5 minutes, is a necessary operating procedure when resolving a mismatched solution produced by the SE. The EMS engineer determined that the mismatch in the SE solution was due to the SE model depicting Cinergy's Bloomington-Denois Creek 230-kV line as being in service, when it had actually been out of service since 12:12 EDT.
- ◆ At 13:00 EDT, after making the appropriate changes to the SE model and manually triggering the SE, the MISO EMS engineer achieved two valid solutions.
- ◆ At 13:30 EDT, the MISO EMS engineer went to lunch. He forgot to re-engage the automatic periodic trigger.
- ◆ At 14:14 EDT, FirstEnergy's "Alarm and Event Processing Routine" (AEPR)-a key software program that gives operators visual and audible indications of events occurring on their portion of the grid-began to malfunction. FirstEnergy system operators were unaware that the software was not functioning properly. This software did not become functional again until much later that evening.
- ◆ At 14:40 EDT, an Ops engineer discovered that the SE was not solving. He went to notify an EMS engineer.
- ◆ At 14:41 EDT, FirstEnergy's server running the AEPR software failed to the backup server. Control room staff remained unaware that the AEPR software was not functioning properly.
- ◆ At 14:44 EDT, an MISO EMS engineer, after being alerted by the Ops engineer, reactivated the automatic periodic trigger and, for speed, manually triggered the program. The SE program again showed a mismatch.
- ◆ At 14:54 EDT, FirstEnergy's backup server failed. AEPR continued to malfunction. The Area Control Error (ACE) calculations and Strip Charting routines malfunctioned, and the dispatcher user interface slowed significantly.
- ◆ At 15:00 EDT, FirstEnergy used its emergency backup system to control the system and make ACE calculations. ACE calculations and control systems continued to run on the emergency backup system until roughly 15:08 EDT, when the primary server was restored.
- ◆ At 15:05 EDT, FirstEnergy's Harding-Chamberlin 345-kV line tripped and locked out. FE system operators did not receive notification from the AEPR software, which continued to malfunction, unbeknownst to the FE system operators.
- ◆ At 15:08 EDT, using data obtained at roughly 15:04 EDT (it takes about 5 minutes for the SE to provide a result), the MISO EMS engineer concluded that the SE mismatched due to a line outage. His experience allowed him to isolate the outage to the Stuart-Atlanta 345-kV line (which tripped about an hour earlier, at 14:02 EDT). He took the Stuart-Atlanta line out of service in the SE model and got a valid solution.
- ◆ Also at 15:08 EDT, the FirstEnergy primary server was restored. ACE calculations and control systems were now running on the primary server. AEPR continued to malfunction, unbeknownst to the FirstEnergy system operators.
- ◆ At 15:09 EDT, the MISO EMS engineer went to the control room to tell the operators that he thought the Stuart-Atlanta line was out of service. Control room operators referred to their



“Outage Scheduler” and informed the EMS engineer that their data showed the Stuart-Atlanta line was “up” and that the EMS engineer should depict the line as in service in the SE model. At 15:17 EDT, the EMS engineer ran the SE with the Stuart-Atlanta line “live.” The model again mismatched.

- ◆ At 15:29 EDT, the MISO EMS Engineer asked MISO operators to call the PJM Interconnect to determine the status of the Stuart-Atlanta line. MISO was informed that the Stuart-Atlanta line had tripped at 14:02 EDT. The EMS engineer adjusted the model, which by that time had been updated with the 15:05 EDT Harding-Chamberlin 345-kV line trip, and came up with a valid solution.
- ◆ At 15:32 EDT, FirstEnergy’s Hanna-Juniper 345-kV line tripped and locked out. The AEPR continued to malfunction.
- ◆ At 15:41 EDT, the lights flickered at FirstEnergy’s control facility, because the facility had lost grid power and switched over to its emergency power supply.
- ◆ At 15:42 EDT, a FirstEnergy dispatcher realized that the AEPR was not working and informed technical support staff of the problem.

## Findings to Date

The SWG has developed the following findings via analysis of collected data and discussions with energy companies and entities identified by the ESWG as pertinent to the SWG’s analysis. SWG analysis to date provides no evidence that malicious actors—either individuals or organizations—are responsible for, or contributed to, the power outage of August 14, 2003. The SWG continues to coordinate closely with the other Task Force Working Groups and members of the U.S. and Canadian law enforcement and DHS/OCIPEP communities to collect and analyze data to test this preliminary finding.

No intelligence reports before, during, or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature related to the sector, which was provided to the North American energy industry by

U.S. and Canadian government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack against oil production facilities, power plants, or nuclear plants on the U.S. East Coast during the summer of 2003. The type of physical attack described in the intelligence that prompted the threat information was not consistent with the events of the power outage.

Although there were a number of worms and viruses impacting the Internet and Internet-connected systems and networks in North America before and during the outage, the SWG’s preliminary analysis provides no indication that worm/virus activity had a significant effect on the power generation and delivery systems. Further SWG analysis will test this finding.

SWG analysis to date suggests that failure of a software program—not linked to malicious activity—may have contributed significantly to the power outage of August 14, 2003. Specifically, key personnel may not have been aware of the need to take preventive measures at critical times, because an alarm system was malfunctioning. The SWG continues to work closely with the operators of the affected system to determine the nature and scope of the failure, and whether similar software failures could create future system vulnerabilities. The SWG is in the process of engaging system vendors and operators to determine whether any technical or process-related modifications should be implemented to improve system performance in the future.

The existence of both internal and external links from SCADA systems to other systems introduced vulnerabilities. At this time, however, preliminary analysis of information derived from interviews with operators provides no evidence indicating exploitation of these vulnerabilities before or during the outage. Future SWG work will provide greater insight into this issue.

Analysis of information derived from interviews with operators suggests that, in some cases, visibility into the operations of surrounding areas was lacking. Some companies appear to have had only a limited understanding of the status of the electric systems outside their immediate control. This may have been, in part, the result of a failure to use modern dynamic mapping and data sharing systems. Future SWG work will clarify this issue.





## Appendix A

# Description of Outage Investigation and Plan for Development of Recommendations

On August 14, 2003, the northeastern U.S. and Ontario, Canada, suffered one of the largest power blackouts in the history of North America. The area affected extended from New York, Massachusetts, and New Jersey west to Michigan, and from Ohio north to Ontario.

This appendix outlines the process used to investigate why the blackout occurred and was not contained, and explains how recommendations will be developed to prevent and minimize the scope of future outages. The essential first step in the process was the creation of a joint U.S.-Canada Power System Outage Task Force to provide oversight for the investigation and the development of recommendations.

### Task Force Composition and Responsibilities

President George W. Bush and Prime Minister Jean Chrétien created the joint Task Force to identify the causes of the August 14, 2003 power outage and to develop recommendations to prevent and contain future outages. The co-chairs of the Task Force are U.S. Secretary of Energy Spencer Abraham and Minister of Natural Resources Canada Herb Dhaliwal. Other U.S. members are Nils J. Diaz, Chairman of the Nuclear Regulatory Commission, Tom Ridge, Secretary of Homeland Security, and Pat Wood, Chairman of the Federal Energy Regulatory Commission. The other Canadian members are Deputy Prime Minister John Manley, Linda J. Keen, President and CEO of the Canadian Nuclear Safety Commission, and Kenneth Vollman, Chairman of the National Energy Board. The coordinators for the Task Force are Jimmy Glotfelty on behalf of the U.S. Department of Energy and Dr. Nawal Kamel on behalf of Natural Resources Canada.

U.S. Energy Secretary Spencer Abraham and Minister of Natural Resources Canada Herb Dhaliwal met in Detroit, Michigan on August 20, and agreed on an outline for the Task Force's activities. The outline directed the Task Force to divide its efforts into two phases. The first phase was to focus on what caused the outage and why it was not contained, and the second was to focus on the

development of recommendations to prevent and minimize future power outages. On August 27, Secretary Abraham and Minister Dhaliwal announced the formation of three Working Groups to support the work of the Task Force. The three Working Groups address electric system issues, security matters, and questions related to the performance of nuclear power plants over the course of the outage. The members of the Working Groups are officials from relevant federal departments and agencies, technical experts, and senior representatives from the affected states and the Province of Ontario.

### U.S.-Canada-NERC Investigation Team

Under the oversight of the Task Force, a team of electric system experts was established to investigate the causes of the outage. This team was comprised of individuals from several U.S. federal agencies, the U.S. Department of Energy's national laboratories, Canadian electric industry, Canada's National Energy Board, staff from the North American Electric Reliability Council (NERC), and the U.S. electricity industry. The overall investigative team was divided into several analytic groups with specific responsibilities, including data management, determining the sequence of outage events, system modeling, evaluation of operating tools and communications, transmission system performance, generator performance, vegetation and right-of-way management, transmission and reliability investments, and root cause analysis. The root cause analysis is best understood as an analytic framework as opposed to a stand-alone analytic effort. Its function was to enable the analysts to draw upon and organize information from all of the other analyses, and by means of a rigorously logical and systematic procedure, assess alternative hypotheses and identify the root causes of the outage.

Separate teams were established to address issues related to the performance of nuclear power plants affected by the outage, and physical and cyber security issues related to the bulk power infrastructure.

## Function of the Working Groups

The U.S. and Canadian co-chairs of each of the three Working Groups (i.e., an Electric System Working Group, a Nuclear Working Group, and a Security Working Group) designed various work products to be prepared by the investigative teams. Drafts of these work products were reviewed and commented upon by the relevant Working Groups. These work products were then synthesized into a single Interim Report reflecting the conclusions of the three investigative teams and the Working Groups. Determination of when the Interim Report was complete and appropriate for release to the public was the responsibility of the joint Task Force.

## Confidentiality of Data and Information

Given the seriousness of the blackout and the importance of averting or minimizing future blackouts, it was essential that the Task Force's teams have access to pertinent records and data from the regional independent system operators (ISOs) and electric companies affected by the blackout, and for the investigative team to be able to interview appropriate individuals to learn what they saw and knew at key points in the evolution of the outage, what actions they took, and with what purpose. In recognition of the sensitivity of this information, Working Group members and members of the teams signed agreements affirming that they would maintain the confidentiality of data and information provided to them, and refrain from independent or premature statements to the media or the public about the activities, findings, or conclusions of the individual Working Groups or the Task Force as a whole.

## Relevant U.S. and Canadian Legal Framework

### *United States*

The Secretary of Energy directed the Department of Energy (DOE) to gather information and conduct an investigation to examine the cause or causes of the August 14, 2003 blackout. In initiating this effort, the Secretary exercised his authority, including section 11 of the Energy Supply and Environmental Coordination Act of 1974, and section 13 of the Federal Energy Administration Act of 1974, to gather energy-related information and conduct investigations. This authority gives him and the DOE the ability to collect such energy information as he deems necessary to assist in the

formulation of energy policy, to conduct investigations at reasonable times and in a reasonable manner, and to conduct physical inspections at energy facilities and business premises. In addition, DOE can inventory and sample any stock of fuels or energy sources therein, inspect and copy records, reports, and documents from which energy information has been or is being compiled and to question such persons as it deems necessary. DOE worked closely with the Canadian Department of Natural Resources and NERC on the investigation.

### *Canada*

Minister Dhaliwal, as the Minister responsible for Natural Resources Canada, was appointed by Prime Minister Chrétien as the Canadian Co-Chair of the Task Force. Minister Dhaliwal works closely with his American Co-Chair, Secretary of Energy Abraham, as well as NERC and his provincial counterparts in carrying out his responsibilities. The Task Force will report to the Prime Minister and the US President upon the completion of its mandate.

Under Canadian law, the Task Force is characterized as a non-statutory, advisory body that does not have independent legal personality. The Task Force does not have any power to compel evidence or witnesses, nor is it able to conduct searches or seizures. In Canada, the Task Force will rely on voluntary disclosure for obtaining information pertinent to its work.

## Investigative Process

### *Collection of Data and Information from ISOs, Utilities, States, and the Province of Ontario*

On Tuesday, August 19, 2003, investigators affiliated with the U.S. Department of Energy (USDOE) began interviewing control room operators and other key officials at the ISOs and the companies most directly involved with the initial stages of the outage. In addition to the information gained in the interviews, the interviewers sought information and data about control room operations and practices, the organization's system status and conditions on August 14, the organization's operating procedures and guidelines, load limits on its system, emergency planning and procedures, system security analysis tools and procedures, and practices for voltage and frequency monitoring. Similar interviews were held later with staff at Ontario's Independent Electricity Market Operator (IMO) and Hydro One in Canada.

On August 22 and 26, NERC directed the reliability coordinators at the ISOs to obtain a wide range of data and information from the control area coordinators under their oversight. The data requested included System Control and Data Acquisition (SCADA) logs, Energy Management System (EMS) logs, alarm logs, data from local digital fault recorders, data on transmission line and generator “trips” (i.e., automatic disconnection to prevent physical damage to equipment), state estimator data, operator logs and transcripts, and information related to the operation of capacitors, phase shifting transformers, load shedding, static var compensators, special protection schemes or stability controls, and high-voltage direct current (HVDC) facilities. NERC issued another data request to FirstEnergy on September 15 for copies of studies since 1990 addressing voltage support, reactive power supply, static capacitor applications, voltage requirements, import or transfer capabilities (in relation to reactive capability or voltage levels), and system impacts associated with unavailability of the Davis-Besse plant. All parties were instructed that data and information provided to either DOE or NERC did not have to be submitted a second time to the other entity—all material provided would go into a common data base.

The investigative team held three technical conferences (August 22, September 8-9, and October 1-3) with the ISOs and key utilities aimed at clarifying the data received, filling remaining gaps in the data, and developing a shared understanding of the data’s implications. The team also requested information from the public utility commissions in the affected states and Ontario on transmission right-of-way maintenance, transmission planning, and the scope of any state-led investigations concerning the August 14 blackout. The team also commissioned a study by a firm specializing in utility vegetation management to identify “best practices” concerning such management in right of way areas and to use those practices in gauging the performance of companies who had lines go out of service on August 14 due to tree contact.

### ***Data “Warehouse”***

The data collected by the investigative team became voluminous, so an electronic repository capable of storing thousands of transcripts, graphs, generator and transmission data and reports was constructed in Princeton, NJ at the NERC headquarters. At present the data base is over 20 Gigabytes of information. That data

consists of over 10,000 different files some of which contain multiple files. The objective was to establish a set of validated databases that the several analytic teams could access independently on an as-needed basis.

The following are the information sources for the Electric System Investigation:

- ◆ Interviews conducted by members of the U.S.-Canada Electric Power System Outage Investigation Team with personnel at all of the utilities, control areas and reliability coordinators in the weeks following the blackout.
- ◆ Three fact-gathering meetings conducted by the Investigation Team with personnel from the above organizations on August 22, September 8 and 9, and October 1 to 3, 2003.
- ◆ Materials provided by the above organizations in response to one or more data requests from the Investigation Team.
- ◆ Extensive review of all taped phone transcripts between involved operations centers.
- ◆ Additional interviews and field visits with operating personnel on specific issues in October, 2003.
- ◆ Field visits to examine transmission lines and vegetation at short-circuit locations.
- ◆ Materials provided by utilities and state regulators in response to data requests on vegetation management issues.
- ◆ Detailed examination of thousands of individual relay trips for transmission and generation events.
- ◆ Computer simulation and modeling conducted by groups of experts from utilities, reliability coordinators, reliability councils, and the U.S. and Canadian governments.

### ***Sequence of Events***

Establishing a precise and accurate sequence of outage-related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time-stamped, there was some variance from source to source in how the time-stamping was done, and not all of the time-stamps were synchronized to the National Institute of Standards and Technology (NIST) standard clock in Boulder, CO. Validating the timing of specific events



became a large, important, and sometimes difficult task. This work was also critical to the issuance by the Task Force on September 12 of a “timeline” for the outage. The timeline briefly described the principal events, in sequence, leading up to the initiation of the outage’s cascade phase, and then in the cascade itself. The timeline was not intended, however, to address the causal relationships among the events described, or to assign fault or responsibility for the blackout. All times in the chronology are in Eastern Daylight Time.

### ***System Modeling and Simulation Analysis***

The system modeling and simulation team replicated system conditions on August 14 and the events leading up to the blackout. While the sequence of events provides a precise description of discrete events, it does not describe the overall state of the electric system and how close it was to various steady-state, voltage stability, and power angle stability limits. An accurate computer model of the system, benchmarked to actual conditions at selected critical times on August 14, allowed analysts to conduct a series of sensitivity studies to determine if the system was stable and within limits at each point in time leading up to the cascade. The analysis also confirmed when the system became unstable, and allowed analysts to test whether measures such as load-shedding would have prevented the cascade.

This team consisted of a number of NERC staff and persons with expertise in areas necessary to read and interpret all of the data logs, digital fault recorder information, sequence of events recorders information, etc. The team consisted of about 36 people involved at various different times with additional experts from the affected areas to understand the data.

### ***Assessment of Operations Tools, SCADA/EMS, Communications, and Operations Planning***

The Operations Tools, SCADA/EMS, Communications, and Operations Planning Team assessed the observability of the electric system to operators and reliability coordinators, and the availability and effectiveness of operational (real-time and day-ahead) reliability assessment tools, including redundancy of views and the ability to observe the “big picture” regarding bulk electric system conditions. The team investigated operating practices and effectiveness of operating entities and reliability coordinators in the affected area. This team investigated all aspects of the blackout related to

operator and reliability coordinator knowledge of system conditions, action or inactions, and communications.

### ***Frequency/ACE Analysis***

The Frequency/ACE Team analyzed potential frequency anomalies that may have occurred on August 14, as compared to typical interconnection operations. The team also determined whether there were any unusual issues with control performance and frequency and any effects they may have had related to the cascading failure, and whether frequency related anomalies were contributing factors or symptoms of other problems leading to the cascade.

### ***Assessment of Transmission System Performance, Protection, Control, Maintenance, and Damage***

This team investigated the causes of all transmission facility automatic operations (trips and reclosings) leading up to and through to the end of the cascade on all facilities greater than 100 kV. Included in the review were relay protection and remedial action schemes and identification of the cause of each operation and any misoperations that may have occurred. The team also assessed transmission facility maintenance practices in the affected area as compared to good utility practice and identified any transmission equipment that was damaged in any way as a result of the cascading outage. The team reported patterns and conclusions regarding what caused transmission facilities to trip; why did the cascade extend as far as it did and not further into other systems; any misoperations and the effect those misoperations had on the outage; and any transmission equipment damage. Also the team reported on the transmission facility maintenance practices of entities in the affected area compared to good utility practice.

### ***Assessment of Generator Performance, Protection, Controls, Maintenance, and Damage***

This team investigated the cause of generator trips for all generators with a 10 MW or greater nameplate rating leading to and through the end of the cascade. The review included the cause for the generator trips, relay targets, unit power runbacks, and voltage/reactive power excursions. The team reported any generator equipment that was damaged as a result of the cascading outage. The team reported on patterns and conclusions regarding what caused generation facilities to trip. The team



identified any unexpected performance anomalies or unexplained events. The team assessed generator maintenance practices in the affected area as compared to good utility practice. The team analyzed the coordination of generator under-frequency settings with transmission settings, such as under-frequency load shedding. The team gathered and analyzed data on affected nuclear units and worked with the Nuclear Regulatory Commission to address U.S. nuclear unit issues.

**Assessment of Right of Way (ROW) Maintenance**

The Vegetation/ROW Team investigated the practices of transmission facilities owners in the affected areas for vegetation management and ROW maintenance. These practices were compared to accepted utility practices in general across the Eastern Interconnection. Also, the team investigated historical patterns in the area related to outages caused by contact with vegetation.

**Root Cause Analysis**

The investigation team used an analytic technique called root cause analysis to help guide the overall investigation process by providing a systematic

approach to evaluating root causes and contributing factors leading to the start of the cascade on August 14. The root cause analysis team worked closely with the technical investigation teams providing feedback and queries on additional information. Also, drawing on other data sources as needed, the root cause analysis verified facts regarding conditions and actions (or inactions) that contributed to the blackout.

**Oversight and Coordination**

The Task Force’s U.S. and Canadian coordinators held frequent conference calls to ensure that all components of the investigation were making timely progress. They briefed both Secretary Abraham and Minister Dhaliwal regularly and provided weekly summaries from all components on the progress of the investigation. The leadership of the electric system investigation team held daily conference calls to address analytical and process issues through the investigation. The three Working Groups held weekly conference calls to enable the investigation team to update the Working Group members on the state of the overall analysis.

**Root Cause Analysis**

Root cause analysis is a systematic approach to identifying and validating causal linkages among conditions, events, and actions (or inactions) leading up to a major event of interest—in this case the August 14 blackout. It has been successfully applied in investigations of events such as nuclear power plant incidents, airplane crashes, and the recent Columbia space shuttle disaster.

Root cause analysis is driven by facts and logic. Events and conditions that may have helped to cause the major event in question must be described in factual terms. Causal linkages must be established between the major event and earlier conditions or events. Such earlier conditions or events must be examined in turn to determine their causes, and at each stage the investigators must ask whether a particular condition or event could have developed or occurred if a proposed cause (or combination of causes) had not been

present. If the particular event being considered could have occurred without the proposed cause (or combination of causes), the proposed cause or combination of causes is dropped from consideration and other possibilities are considered.

Root cause analysis typically identifies several or even many causes of complex events; each of the various branches of the analysis is pursued until either a “root cause” is found or a non-correctable condition is identified. (A condition might be considered as non-correctable due to existing law, fundamental policy, laws of physics, etc.). Sometimes a key event in a causal chain leading to the major event could have been prevented by timely action by one or another party; if such action was feasible, and if the party had a responsibility to take such action, the failure to do so becomes a root cause of the major event.



## Appendix B

### List of Electricity Acronyms

BPA	Bonneville Power Administration
CNSC	Canadian Nuclear Safety Commission
DOE	Department of Energy (U.S.)
ECAR	East Central Area Reliability Coordination Agreement
ERCOT	Electric Reliability Council of Texas
FERC	Federal Energy Regulatory Commission (U.S.)
FRCC	Florida Reliability Coordinating Council
GW, GWh	Gigawatt, Gigawatt-hour
kV, kVAr	Kilovolt, Kilovolt-amperes-reactive
kW, kWh	Kilowatt, Kilowatt-hour
MAAC	Mid-Atlantic Area Council
MAIN	Mid-America Interconnected Network
MAPP	Mid-Continent Area Power Pool
MVA, MVA <sub>r</sub>	Megavolt-amperes, Megavolt-amperes-reactive
MW, MWh	Megawatt, Megawatt-hour
NERC	North American Electric Reliability Council
NPCC	Northeast Power Coordination Council
NRC	Nuclear Regulatory Commission (U.S.)
NRCan	Natural Resources Canada
OTD	Office of Transmission and Distribution (U.S. DOE)
PUC	Public Utility Commission (state)
RTO	Regional Transmission Organization
SERC	Southeast Electric Reliability Council
SPP	Southwest Power Pool
TVA	Tennessee Valley Authority (U.S.)





## Appendix C

# Electricity Glossary

**AC:** Alternating current; current that changes periodically (sinusoidally) with time.

**ACE:** Area Control Error in MW. A negative value indicates a condition of under-generation relative to system load and imports, and a positive value denotes over-generation.

**Active Power:** Also known as “real power.” The rate at which work is performed or that energy is transferred. Electric power is commonly measured in watts or kilowatts. The terms “active” or “real” power are often used in place of the term power alone to differentiate it from reactive power. The rate of producing, transferring, or using electrical energy, usually expressed in kilowatts (kW) or megawatts (MW).

**Adequacy:** The ability of the electric system to supply the aggregate electrical demand and energy requirements of customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.

**AGC:** Automatic Generation Control is a computation based on measured frequency and computed economic dispatch. Generation equipment under AGC automatically respond to signals from an EMS computer in real time to adjust power output in response to a change in system frequency, tie-line loading, or to a prescribed relation between these quantities. Generator output is adjusted so as to maintain a target system frequency (usually 60 Hz) and any scheduled MW interchange with other areas.

**Apparent Power:** The product of voltage and current phasors. It comprises both active and reactive power, usually expressed in kilovoltamperes (kVA) or megavoltamperes (MVA).

**Automatic Operating Systems:** Special protection systems, or remedial action schemes, that require no intervention on the part of system operators.

**Blackstart Capability:** The ability of a generating unit or station to go from a shutdown condition to an operating condition and start delivering power without assistance from the electric system.

**Bulk Electric System:** A term commonly applied to the portion of an electric utility system that

encompasses the electrical generation resources and bulk transmission system.

**Bulk Transmission:** A functional or voltage classification relating to the higher voltage portion of the transmission system, specifically, lines at or above a voltage level of 115 kV.

**Bus:** Shortened from the word busbar, meaning a node in an electrical network where one or more elements are connected together.

**Capacitor Bank:** A capacitor is an electrical device that provides reactive power to the system and is often used to compensate for reactive load and help support system voltage. A bank is a collection of one or more capacitors at a single location.

**Capacity:** The rated continuous load-carrying ability, expressed in megawatts (MW) or megavolt-amperes (MVA) of generation, transmission, or other electrical equipment.

**Cascading:** The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread service interruption, which cannot be restrained from sequentially spreading beyond an area predetermined by appropriate studies.

**Circuit:** A conductor or a system of conductors through which electric current flows.

**Circuit Breaker:** A switching device connected to the end of a transmission line capable of opening or closing the circuit in response to a command, usually from a relay.

**Control Area:** An electric power system or combination of electric power systems to which a common automatic control scheme is applied in order to: (1) match, at all times, the power output of the generators within the electric power system(s) and capacity and energy purchased from entities outside the electric power system(s), with the load in the electric power system(s); (2) maintain, within the limits of Good Utility Practice, scheduled interchange with other Control Areas; (3) maintain the frequency of the electric power system(s) within reasonable limits in accordance with Good Utility Practice; and (4) provide sufficient

generating capacity to maintain operating reserves in accordance with Good Utility Practice.

**Contingency:** The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element. A contingency also may include multiple components, which are related by situations leading to simultaneous component outages.

**Control Area Operator:** An individual or organization responsible for controlling generation to maintain interchange schedule with other control areas and contributing to the frequency regulation of the interconnection. The control area is an electric system that is bounded by interconnection metering and telemetry.

**Current (Electric):** The rate of flow of electrons in an electrical conductor measured in Amperes.

**DC:** Direct current; current that is steady and does not change with time.

**Dispatch Operator:** Control of an integrated electric system involving operations such as assignment of levels of output to specific generating stations and other sources of supply; control of transmission lines, substations, and equipment; operation of principal interties and switching; and scheduling of energy transactions.

**Distribution Network:** The portion of an electric system that is dedicated to delivering electric energy to an end user, at or below 69 kV. The distribution network consists primarily of low-voltage lines and transformers that “transport” electricity from the bulk power system to retail customers.

**Disturbance:** An unplanned event that produces an abnormal system condition.

**Electrical Energy:** The generation or use of electric power by a device over a period of time, expressed in kilowatthours (kWh), megawatthours (MWh), or gigawatthours (GWh).

**Electric Utility Corporation:** Person, agency, authority, or other legal entity or instrumentality that owns or operates facilities for the generation, transmission, distribution, or sale of electric energy primarily for use by the public, and is defined as a utility under the statutes and rules by which it is regulated. An electric utility can be investor-owned, cooperatively owned, or government-owned (by a federal agency, crown corporation, State, provincial government, municipal government, and public power district).

**Emergency:** Any abnormal system condition that requires automatic or immediate manual action to prevent or limit loss of transmission facilities or generation supply that could adversely affect the reliability of the electric system.

**Emergency Voltage Limits:** The operating voltage range on the interconnected systems that is acceptable for the time, sufficient for system adjustments to be made following a facility outage or system disturbance.

**EMS:** An Energy Management System is a computer control system used by electric utility dispatchers to monitor the real time performance of various elements of an electric system and to control generation and transmission facilities.

**Fault:** A fault usually means a short circuit, but more generally it refers to some abnormal system condition. Faults occur as random events, usually an act of nature.

**Federal Energy Regulatory Commission (FERC):** Independent Federal agency within the U.S. Department of Energy that, among other responsibilities, regulates the transmission and wholesale sales of electricity in interstate commerce.

**Flashover:** A plasma arc initiated by some event such as lightning. Its effect is a short circuit on the network.

**Flowgate:** A single or group of transmission elements intended to model MW flow impact relating to transmission limitations and transmission service usage.

**Forced Outage:** The removal from service availability of a generating unit, transmission line, or other facility for emergency reasons or a condition in which the equipment is unavailable due to unanticipated failure.

**Frequency:** The number of complete alternations or cycles per second of an alternating current, measured in Hertz. The standard frequency in the United States is 60 Hz. In some other countries the standard is 50 Hz.

**Frequency Deviation or Error:** A departure from scheduled frequency. The difference between actual system frequency and the scheduled system frequency.

**Frequency Regulation:** The ability of a Control Area to assist the interconnected system in maintaining scheduled frequency. This assistance can include both turbine governor response and automatic generation control.

**Frequency Swings:** Constant changes in frequency from its nominal or steady-state value.

**Generation (Electricity):** The process of producing electrical energy from other forms of energy; also, the amount of electric energy produced, usually expressed in kilowatt hours (kWh) or megawatt hours (MWh).

**Generator:** Generally, an electromechanical device used to convert mechanical power to electrical power.

**Grid:** An electrical transmission and/or distribution network.

**Grid Protection Scheme:** Protection equipment for an electric power system, consisting of circuit breakers, certain equipment for measuring electrical quantities (e.g., current and voltage sensors) and devices called relays. Each relay is designed to protect the piece of equipment it has been assigned from damage. The basic philosophy in protection system design is that any equipment that is threatened with damage by a sustained fault is to be automatically taken out of service.

**Ground:** A conducting connection between an electrical circuit or device and the earth. A ground may be intentional, as in the case of a safety ground, or accidental, which may result in high overcurrents.

**Imbalance:** A condition where the generation and interchange schedules do not match demand.

**Impedance:** The total effects of a circuit that oppose the flow of an alternating current consisting of inductance, capacitance, and resistance. It can be quantified in the units of ohms.

**Independent System Operator (ISO):** An organization responsible for the reliable operation of the power grid under its purview and for providing open transmission access to all market participants on a nondiscriminatory basis. An ISO is usually not-for-profit and can advise other utilities within its territory on transmission expansion and maintenance but does not have the responsibility to carry out the functions.

**Interchange:** Electric power or energy that flows across tie-lines from one entity to another, whether scheduled or inadvertent.

**Interconnected System:** A system consisting of two or more individual electric systems that normally operate in synchronism and have connecting tie lines.

**Interconnection:** When capitalized, any one of the five major electric system networks in North America: Eastern, Western, ERCOT (Texas), Québec, and Alaska. When not capitalized, the facilities that connect two systems or Control Areas. Additionally, an interconnection refers to the facilities that connect a nonutility generator to a Control Area or system.

**Interface:** The specific set of transmission elements between two areas or between two areas comprising one or more electrical systems.

**Island:** A portion of a power system or several power systems that is electrically separated from the interconnection due to the disconnection of transmission system elements.

**Kilovar (kVAr):** Unit of alternating current reactive power equal to 1,000 VARs.

**Kilovolt (kV):** Unit of electrical potential equal to 1,000 Volts.

**Kilovolt-Amperes (kVA):** Unit of apparent power equal to 1,000 volt amperes. Here, apparent power is in contrast to real power. On ac systems the voltage and current will not be in phase if reactive power is being transmitted.

**Kilowatthour (kWh):** Unit of energy equaling one thousand watthours, or one kilowatt used over one hour. This is the normal quantity used for metering and billing electricity customers. The price for a kWh varies from approximately 4 cents to 15 cents. At a 100% conversion efficiency, one kWh is equivalent to about 4 fluid ounces of gasoline, 3/16 pound of liquid petroleum, 3 cubic feet of natural gas, or 1/4 pound of coal.

**Line Trip:** Refers to the automatic opening of the conducting path provided by a transmission line by the circuit breakers. These openings or “trips” are designed to protect the transmission line during faulted conditions.

**Load (Electric):** The amount of electric power delivered or required at any specific point or points on a system. The requirement originates at the energy-consuming equipment of the consumers. Load should not be confused with demand, which is the measure of power that a load receives or requires. See “Demand.”

**Load Shedding:** The process of deliberately removing (either manually or automatically) pre-selected customer demand from a power system in response to an abnormal condition, to maintain the integrity of the system and minimize overall customer outages.



**Lockout:** A state of a transmission line following breaker operations where the condition detected by the protective relaying was not eliminated by temporarily opening and reclosing the line, possibly multiple times. In this state, the circuit breakers cannot generally be reclosed without resetting a lockout device.

**Market Participant:** An entity participating in the energy marketplace by buying/selling transmission rights, energy, or ancillary services into, out of, or through an ISO-controlled grid.

**Megawatthour (MWh):** One million watthours.

**NERC Interregional Security Network (ISN):** A communications network used to exchange electric system operating parameters in near real time among those responsible for reliable operations of the electric system. The ISN provides timely and accurate data and information exchange among reliability coordinators and other system operators. The ISN, which operates over the frame relay NERCnet system, is a private Intranet that is capable of handling additional applications between participants.

**Normal (Precontingency) Operating Procedures:** Operating procedures that are normally invoked by the system operator to alleviate potential facility overloads or other potential system problems in anticipation of a contingency.

**Normal Voltage Limits:** The operating voltage range on the interconnected systems that is acceptable on a sustained basis.

**North American Electric Reliability Council (NERC):** A not-for-profit company formed by the electric utility industry in 1968 to promote the reliability of the electricity supply in North America. NERC consists of nine Regional Reliability Councils and one Affiliate, whose members account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. The members of these Councils are from all segments of the electricity supply industry: investor-owned, federal, rural electric cooperative, state/municipal, and provincial utilities, independent power producers, and power marketers. The NERC Regions are: East Central Area Reliability Coordination Agreement (ECAR); Electric Reliability Council of Texas (ERCOT); Mid-Atlantic Area Council (MAAC); Mid-America Interconnected Network (MAIN); Mid-Continent Area Power Pool (MAPP); Northeast Power Coordinating Council (NPCC);

Southeastern Electric Reliability Council (SERC); Southwest Power Pool (SPP); Western Systems Coordinating Council (WSCC); and Alaskan Systems Coordination Council (ASCC, Affiliate).

**Operating Criteria:** The fundamental principles of reliable interconnected systems operation, adopted by NERC.

**Operating Guides:** Operating practices that a Control Area or systems functioning as part of a Control Area may wish to consider. The application of Guides is optional and may vary among Control Areas to accommodate local conditions and individual system requirements.

**Operating Policies:** The doctrine developed for interconnected systems operation. This doctrine consists of Criteria, Standards, Requirements, Guides, and instructions, which apply to all Control Areas.

**Operating Procedures:** A set of policies, practices, or system adjustments that may be automatically or manually implemented by the system operator within a specified time frame to maintain the operational integrity of the interconnected electric systems.

**Operating Requirements:** Obligations of a Control Area and systems functioning as part of a Control Area.

**Operating Standards:** The obligations of a Control Area and systems functioning as part of a Control Area that are measurable. An Operating Standard may specify monitoring and surveys for compliance.

**Outage:** The period during which a generating unit, transmission line, or other facility is out of service.

**Post-contingency Operating Procedures:** Operating procedures that may be invoked by the system operator to mitigate or alleviate system problems after a contingency has occurred.

**Protective Relay:** A device designed to detect abnormal system conditions, such as electrical shorts on the electric system or within generating plants, and initiate the operation of circuit breakers or other control equipment.

**Power/Phase Angle:** The angular relationship between an ac (sinusoidal) voltage across a circuit element and the ac (sinusoidal) current through it. The real power that can flow is related to this angle.



**Power:** See “Active Power.”

**Reactive Power:** The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kVAR) or megavars (MVAR). The mathematical product of voltage and current consumed by reactive loads. Examples of reactive loads include capacitors and inductors. These types of loads, when connected to an ac voltage source, will draw current, but because the current is 90 degrees out of phase with the applied voltage, they actually consume no real power in the ideal sense.

**Real Power:** See “Active Power.”

**Regional Transmission Operator (RTO):** An organization that is independent from all generation and power marketing interests and has exclusive responsibility for electric transmission grid operations, short-term electric reliability, and transmission services within a multi-State region. To achieve those objectives, the RTO manages transmission facilities owned by different companies and encompassing one, large, contiguous geographic area.

**Relay:** A device that controls the opening and subsequent reclosing of circuit breakers. Relays take measurements from local current and voltage transformers, and from communication channels connected to the remote end of the lines. A relay output trip signal is sent to circuit breakers when needed.

**Relay Setting:** The parameters that determine when a protective relay will initiate operation of circuit breakers or other control equipment.

**Reliability:** The degree of performance of the elements of the bulk electric system that results in electricity being delivered to customers within accepted standards and in the amount desired. Reliability may be measured by the frequency, duration, and magnitude of adverse effects on the electric supply. Electric system reliability can be addressed by considering two basic and functional aspects of the electric system Adequacy and Security.

**Reliability Coordinator:** An individual or organization responsible for the safe and reliable

operation of the interconnected transmission system for their defined area, in accordance with NERC reliability standards, regional criteria, and subregional criteria and practices.

**Resistance:** The characteristic of materials to restrict the flow of current in an electric circuit. Resistance is inherent in any electric wire, including those used for the transmission of electric power. Resistance in the wire is responsible for heating the wire as current flows through it and the subsequent power loss due to that heating.

**Restoration:** The process of returning generators and transmission system elements and restoring load following an outage on the electric system.

**Safe Limits:** System limits on quantities such as voltage or power flows such that if the system is operated within these limits it is secure and reliable.

**SCADA:** Supervisory Control and Data Acquisition system; a system of remote control and telemetry used to monitor and control the electric system.

**Scheduling Coordinator:** An entity certified by the ISO for the purpose of undertaking scheduling functions.

**Security:** The ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements.

**Security Coordinator:** An individual or organization that provides the security assessment and emergency operations coordination for a group of Control Areas.

**Short Circuit:** A low resistance connection unintentionally made between points of an electrical circuit, which may result in current flow far above normal levels.

**Single Contingency:** The sudden, unexpected failure or outage of a system facility(s) or element(s) (generating unit, transmission line, transformer, etc.). Elements removed from service as part of the operation of a remedial action scheme are considered part of a single contingency.

**Special Protection System:** An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components.

**Stability:** The ability of an electric system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

**Stability Limit:** The maximum power flow possible through a particular point in the system while maintaining stability in the entire system or the part of the system to which the stability limit refers.

**State Estimator:** Computer software that takes redundant measurements of quantities related to system state as input and provides an estimate of the system state (bus voltage phasors). It is used to confirm that the monitored electric power system is operating in a secure state by simulating the system both at the present time and one step ahead, for a particular network topology and loading condition. With the use of a state estimator and its associated contingency analysis software, system operators can review each critical contingency to determine whether each possible future state is within reliability limits.

**Station:** A node in an electrical network where one or more elements are connected. Examples include generating stations and substations.

**Substation:** Facility equipment that switches, changes, or regulates electric voltage.

**Subtransmission:** A functional or voltage classification relating to lines at voltage levels between 69kV and 115kV.

**Supervisory Control and Data Acquisition (SCADA):** See SCADA.

**Surge:** A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.

**Surge Impedance Loading:** The maximum amount of real power that can flow down a lossless transmission line such that the line does not require any VARs to support the flow.

**Switching Station:** Facility equipment used to tie together two or more electric circuits through switches. The switches are selectively arranged to permit a circuit to be disconnected, or to change the electric connection between the circuits.

**Synchronize:** The process of connecting two previously separated alternating current apparatuses after matching frequency, voltage, phase angles, etc. (e.g., paralleling a generator to the electric system).

**System:** An interconnected combination of generation, transmission, and distribution components comprising an electric utility and independent

power producer(s) (IPP), or group of utilities and IPP(s).

**System Operator:** An individual at an electric system control center whose responsibility it is to monitor and control that electric system in real time.

**System Reliability:** A measure of an electric system's ability to deliver uninterrupted service at the proper voltage and frequency.

**Thermal Limit:** A power flow limit based on the possibility of damage by heat. Heating is caused by the electrical losses which are proportional to the square of the *active power* flow. More precisely, a thermal limit restricts the sum of the squares of *active* and *reactive power*.

**Tie-line:** The physical connection (e.g. transmission lines, transformers, switch gear, etc.) between two electric systems that permits the transfer of electric energy in one or both directions.

**Time Error:** An accumulated time difference between Control Area system time and the time standard. Time error is caused by a deviation in Interconnection frequency from 60.0 Hertz.

**Time Error Correction:** An offset to the Interconnection's scheduled frequency to correct for the time error accumulated on electric clocks.

**Transfer Limit:** The maximum amount of power that can be transferred in a reliable manner from one area to another over all transmission lines (or paths) between those areas under specified system conditions.

**Transformer:** A device that operates on magnetic principles to increase (step up) or decrease (step down) voltage.

**Transient Stability:** The ability of an electric system to maintain synchronism between its parts when subjected to a disturbance of specified severity and to regain a state of equilibrium following that disturbance.

**Transmission:** An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.

**Transmission Loading Relief (TLR):** A procedure used to manage congestion on the electric transmission system.

**Transmission Margin:** The difference between the maximum power flow a transmission line can handle and the amount that is currently flowing on the line.

**Transmission Operator:** NERC-certified person responsible for monitoring and assessing local reliability conditions, who operates the transmission facilities, and who executes switching orders in support of the Reliability Authority.

**Transmission Overload:** A state where a transmission line has exceeded either a normal or emergency rating of the electric conductor.

**Transmission Owner (TO) or Transmission Provider:** Any utility that owns, operates, or controls facilities used for the transmission of electric energy.

**Trip:** The opening of a circuit breaker or breakers on an electric system, normally to electrically isolate a particular element of the system to prevent it from being damaged by fault current or other potentially damaging conditions. See Line Trip for example.

**Voltage:** The electrical force, or “pressure,” that causes current to flow in a circuit, measured in Volts.

**Voltage Collapse (decay):** An event that occurs when an electric system does not have adequate reactive support to maintain voltage stability. Voltage Collapse may result in outage of system elements and may include interruption in service to customers.

**Voltage Control:** The control of transmission voltage through adjustments in generator reactive output and transformer taps, and by switching capacitors and inductors on the transmission and distribution systems.

**Voltage Limits:** A hard limit above or below which is an undesirable operating condition. Normal limits are between 95 and 105 percent of the nominal voltage at the bus under discussion.

**Voltage Reduction:** A procedure designed to deliberately lower the voltage at a bus. It is often used as a means to reduce demand by lowering the customer’s voltage.

**Voltage Stability:** The condition of an electric system in which the sustained voltage level is controllable and within predetermined limits.

**Watt-hour (Wh):** A unit of measure of electrical energy equal to 1 watt of power supplied to, or taken from, an electric circuit steadily for 1 hour.





## Appendix D

### Transmittal Letters from the Three Working Groups

Mr. James W. Glotfelty  
Director, Office of Electric Transmission  
and Distribution  
U.S. Department of Energy  
1000 Independence Avenue SW  
Washington, DC 20585

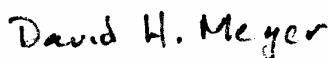
Dr. Nawal Kamel  
Special Assistant to the Deputy Minister  
Natural Resources Canada  
580 Booth Street  
Ottawa, ON  
K1A 0E4

Dear Mr. Glotfelty and Dr. Kamel:

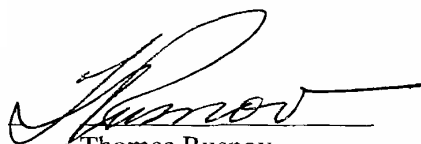
Enclosed is the Interim Report of the Electric System Working Group (ESWG) supporting the United States - Canada Power System Outage Task Force.

This report presents the results of an intensive and thorough investigation by a bi-national team of the causes of the blackout that occurred on August 14, 2003. The report was written largely by four members of the Working Group (Joe Eto, David Meyer, Alison Silverstein, and Tom Rusnov), with important assistance from many members of the Task Force's investigative team. Other members of the ESWG reviewed the report in draft and provided valuable suggestions for its improvement. Those members join us in this submittal and have signed on the attached page. Due to schedule conflicts, one member of the ESWG was not able to participate in the final review of the report and has not signed this transmittal letter for that reason.

Sincerely,



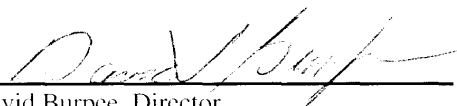
David H. Meyer  
Senior Advisor  
U.S. Department  
of Energy  
Co-Chair, ESWG



Thomas Rusnov  
Senior Advisor  
Natural Resources  
Canada  
Co-Chair, ESWG




Alison Silverstein  
Senior Energy Policy Advisor  
to the Chairman  
Federal Energy Regulatory  
Commission  
Co-Chair, ESWG



David Burpee, Director,  
Renewable and Electrical Energy Division  
Natural Resources Canada




Blaine Loper, Senior Engineer  
Pennsylvania Public Utility Commission




Donald Downes, Chairman  
Connecticut Department of  
Public Utility Control


(not able to participate in review)  
William D. McCarty, Chairman  
Indiana Utility Regulatory Commission



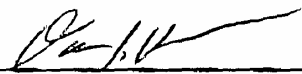
Joseph Eto, Staff Scientist  
U.S. Department of Energy  
Lawrence Berkeley National Laboratory  
Consortium for Electric Reliability  
Technology Solutions



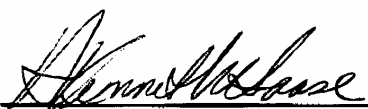
David McFadden  
Chair, National Energy and Infrastructure  
Industry Group  
Gowlings, Lafleur, Henderson LLP  
Ontario




Jeanne Fox, President  
New Jersey Board of Public Utilities




David O'Brien, Commissioner  
Vermont Department of Public Service



H. Kenneth Haase  
Senior Vice President, Transmission  
New York Power Authority



David O'Connor, Commissioner  
Div. of Energy Resources  
Massachusetts Office of Consumer Affairs  
And Business Regulation



Gene Whitney, Policy Analyst  
National Science and Technology Council  
U.S. Office of Science and Technology  
Policy  
Executive Office of the President



Alan Schriber, Chairman  
Ohio Public Utilities Commission



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001



Canadian Nuclear  
Safety Commission

President and  
Chief Executive Officer

Commission canadienne  
de sûreté nucléaire

Présidente et  
première dirigeante

November 5, 2003

**PREDECISIONAL**

Mr. James Glotfelty  
Senior Policy Advisor  
Office of the Secretary  
U.S. Department of Energy  
1000 Independence Ave., Suite 7B-222  
Washington, DC 20585

Dr. Nawal Kamel  
Special Assistant to the Deputy Minister  
Natural Resources Canada  
580 Booth Street  
Ottawa, ON  
K1A 0E4

Dear Mr. Glotfelty and Dr. Kamel:

Enclosed for incorporation into the Task Force report is the interim phase-one report of the Nuclear Working Group supporting the United States - Canada Joint Power System Outage Task Force. The members of the Nuclear Working Group join us in this submittal and have signed the attached pages. This interim report is predecisional (not for public release) until you issue the Task Force interim report, and should be made available only to those individuals needing this information to support the Task Force activities.

Please provide any comments related to the Canadian nuclear plants to either Mr. Jim Blyth (613-995-2655; [blythj@cnsccsn.gc.ca](mailto:blythj@cnsccsn.gc.ca)), or Mark Dallaire (613-947-0957; [dallairem@cnsccsn.gc.ca](mailto:dallairem@cnsccsn.gc.ca)). Comments on the U.S. nuclear plants should be directed to either Mr. Cornelius Holden (301-415-3036; [cfh@nrc.gov](mailto:cfh@nrc.gov)) or Mr John Boska (301-415-2901; [jpb1@nrc.gov](mailto:jpb1@nrc.gov)).

Sincerely,

Nils J. Diaz  
Chairman  
U.S. Nuclear Regulatory Commission  
U.S. Co-chair, Nuclear Working Group

Linda J. Keen  
President and Chief Executive Officer  
Canadian Nuclear Safety Commission  
Canadian Co-chair, Nuclear Working Group

Enclosures: Nuclear Working Group Signature Pages (2)  
Nuclear Working Group Interim Report Phase One

**PREDECISIONAL**

**PREDECISIONAL**

cc w/encl: Mr. James Blyth  
Director General, Reactor Power Regulation  
Canadian Nuclear Safety Commission

Mr. Samuel J. Collins  
Deputy Executive Director, Reactor Programs  
U.S. Nuclear Regulatory Commission

**PREDECISIONAL**



The members of the Nuclear Working Group hereby submit this report as input to the United States - Canada Joint Power System Outage Task Force:



Nils J. Diaz, Chairman  
U.S. Nuclear Regulatory Commission  
Co-chair, Nuclear Working Group




Samuel J. Collins, Deputy Executive Director  
for Reactor Programs  
U.S. Nuclear Regulatory Commission



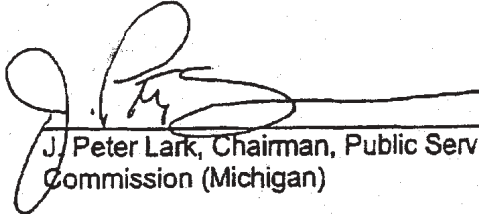
William D. Magwood, IV, Director, Office of  
Nuclear Energy, Science and Technology  
U.S. Department of Energy



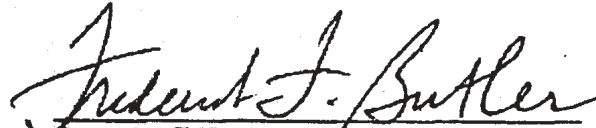
Edward Wilds, Bureau of Air Management,  
Department of Environmental Protection  
(Connecticut)



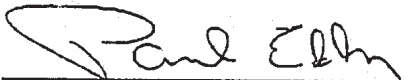
David O'Connor, Commissioner, Division of  
Energy Resources, Office of Consumer  
Affairs and Business Regulation  
(Massachusetts)



J. Peter Lark, Chairman, Public Service  
Commission (Michigan)



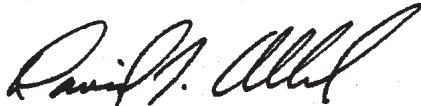
Frederick F. Butler, Commissioner, New  
Jersey Board of Public Utilities (New Jersey)



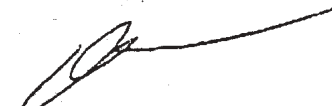
Paul Eddy, Power Systems Operations  
Specialist, Public Service Commission (New  
York)



Dr. G. Ivan Maldonado, Associate Professor,  
Mechanical, Industrial and Nuclear  
Engineering; University of Cincinnati (Ohio)

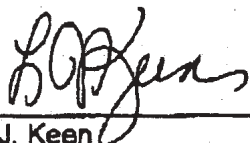


David J. Allard, CHP, Director, Bureau of  
Radiation Protection, Department of  
Environmental Protection (Pennsylvania)



David O'Brien, Commissioner  
Department of Public Service (Vermont)

The members of the Nuclear Working Group hereby submit this report as input to the United States - Canada Joint Power System Outage Task Force:



Linda J. Keen  
President and Chief Executive Officer  
Canadian Nuclear Safety Commission  
Co-chair, Nuclear Working Group



James Blyth  
Director-General, Directorate of Power  
Reactor Regulation  
Canadian Nuclear Safety Commission



Ken Pereira  
Vice-President, Operations Branch  
Canadian Nuclear Safety Commission



Dr. Robert Morrison  
Senior Advisor to the Deputy Minister  
Natural Resources Canada



Duncan Hawthorne  
Chief Executive Officer  
Bruce Power  
(Representing the Province of Ontario)

Mr. James W. Glotfelty  
Director, Office of Electric Transmission  
and Distribution  
U.S. Department of Energy  
1000 Independence Avenue SW  
Washington, DC 20585


Dr. Nawal Kamel  
Special Assistant to the Deputy Minister  
Natural Resources Canada  
580 Booth Street  
Ottawa, ON  
K1A 0E4

Dear Mr. Glotfelty and Dr. Kamel:


Enclosed is the Interim Report of the Security Working Group (SWG) supporting the United States - Canada Power System Outage Task Force.

The SWG Interim Report presents the results of the Working Group's analysis to date of the security aspects of the power outage that occurred on August 14, 2003. This report comprises input from public sector, private sector, and academic members of the SWG, with important assistance from many members of the Task Force's investigative team. As co-chairs of the Security Working Group, we represent all members of the SWG in this submittal and have signed below.

Sincerely,



**Bob Liebowitz**  
Assistant Secretary for  
Infrastructure Protection,  
U.S. Department of Homeland Security  
Co-Chair, SWG



**William S. Elliott**  
Assistant Secretary to the Cabinet,  
Security and Intelligence,  
Privy Council Office  
Government of Canada  
Co-Chair, SWG

Attachment 1:

U.S.-Canada Power System Outage Task Force SWG Steering Committee members:

**Bob Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security (U.S. Government) (Co-Chair)**

**William J.S. Elliott, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office (Government of Canada) (Co-Chair)**

**U.S. Members**

Andy Purdy, Deputy Director, National Cyber Security Division, Department of Homeland Security

Hal Hendershot, Acting Section Chief, Computer Intrusion Section, FBI

Steve Schmidt, Section Chief, Special Technologies and Applications, FBI

Kevin Kolevar, Senior Policy Advisor to the Secretary, DoE

Simon Szykman, Senior Policy Analyst, U.S. Office of Science & Technology Policy, White House

Vincent DeRosa, Deputy Commissioner, Director of Homeland Security (Connecticut)

Richard Swensen, Under-Secretary, Office of Public Safety and Homeland Security (Massachusetts)

Colonel Michael C. McDaniel (Michigan)

Sid Caspersen, Director, Office of Counter-Terrorism (New Jersey)

James McMahon, Senior Advisor (New York)

John Overly, Executive Director, Division of Homeland Security (Ohio)

Arthur Stephens, Deputy Secretary for Information Technology, (Pennsylvania)

Kerry L. Sleeper, Commissioner, Public Safety (Vermont)

**Canada Members**

James Harlick, Assistant Deputy Minister, Office of Critical Infrastructure Protection and Emergency Preparedness

Michael Devaney, Deputy Chief, Information Technology Security Communications Security Establishment

Peter MacAulay, Officer, Technological Crime Branch of the Royal Canadian Mounted Police

Gary Anderson, Chief, Counter-Intelligence – Global, Canadian Security Intelligence Service

Dr. James Young, Commissioner of Public Security, Ontario Ministry of Public Safety and Security